REMARKS/ARGUMENTS

The Applicant has amended claims to clarify that which the Applicant considers to be the invention. The Applicant respectfully submits that amendments to the claim set are fully supported by the originally filed specification.

The amendments to the claims are support specifically by reference to Fig. 6 and the associated description of "protocol 4" beginning at page 47, line 21 of the specification.

In relation to the double patenting rejection a terminal disclaimer is filed in compliance with 37 CFR 1.321(c).

At pages 4-8 of the Office Action, the Examiner rejects claims 1-5, 8-11, 13-18, 21-24 and 27 under 35 USC 102(b) as being anticipated by Bjerrum *et al.* (US 5,311,595).

In the presently claimed invention, independent claims 1 and 14 have been amended to more clearly differentiate the cited prior art document of Bjerrum *et al.* The Examiner considers that the preamble "a consumer authentication protocol for validating the authentcity of an untrusted authentication chip" should not be given patentable weight. The claims are amended to clearly refer to a method and system directed to "a trusted authentication chip", "an untrusted authentication chip", "comparing the decrypted random number and the decrypted data message", and "considering the untrusted chip and the data message to be valid", "otherwise considering the untrusted chip and the data message to be invalid". It is respectfully submitted that the body of the claim clearly is directed to and claims steps or features of an authentication protocol or system for validating the authenticity of an untrusted authentication chip. Bjerrum *et al.* does not disclose or teach a method or system for validating an untrusted authentication chip, rather Bjerrum *et al.* is concerned with the integrity of data transfer between computer systems.

Furthermore, referring specifically to amended claim 1, Bjerrum *et al.* is silent on the step of "comparing the decrypted random number and the decrypted data message with the original random number and the received original data message, without knowledge of the second secret key". The Examiner is reminded that the "decrypted random number" is obtained from a "third encrypted outcome" which in turn is obtained from encrypting a "second decrypted outcome together with an original data message read from the untrusted authentication chip". In contrast, in Bjerrum *et al.* at col. 13, lines 23-31, cards 124 and 224 have been issued together and constitute a coherent set of cards being preprogrammed as regards encryption/decryption algorithms. In the presently claimed invention the "second secret key from the untrusted authentication chip" is not a public key, whereas "the first key from the trusted authentication chip may be a public key".

In the presently claimed invention, only a valid "untrusted authentication chip" would know the value of the "original random number" since the original random number is passed as an encrypted value. Once obtained, the original random number is appended to an original data message and then the result is decrypted. The "trusted authentication chip" can then verify whether the untrusted chip is valid or not. This is not what is disclosed or suggested in Bjerrum *et al.*

In Bjerrum *et al.* authentication requires a complimentary electronic device to interact with the electronic card 124 and 224. Such a requirement is not necessary in the presently claimed invention. Bjerrum *et al.* seeks to establish secure data or document transfer between two computer systems without having to exchange encryption/decryption keys between the systems (col. 2, lines 9-12). Bjerrum *et al.* discloses the requirement to verify that data transferred from the first computer system is identical to the data received at the second computer system (col. 12, lines 35-40). This is a different object of invention to the present invention as defined in independent claims 1 and 14 of the present application. The present invention is not concerned with integrity of transmitted data to which the invention of Bjerrum *et al.* is directed.

Nowhere is the presently claimed authentication protocol or system disclosed, taught or suggested in Bjerrum *et al.* For at least aforementioned reason, it is respectfully submitted that independent amended claims 1 and 14 of the present application are patentable in light of Bjerrum *et al.* and the other prior art documents of record. Likewise, in relation to the 35 USC 103 rejection, the dependent claims of the present application are respectfully submitted to be patentable over Bjerrum *et al.* when taken individually or in combination with any of the other prior art documents of record.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC 102(b) and 35 USC 103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant: SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762